南方电网下属某输电企业自建网以来，对企业信息化的建设一直非常重视，从 2000 年以来，大量的信息系统上线已经对南方电网下属某输电企业的业务带来巨大的效益。作为总部的信息化建设部门，南方电网下属某输电企业信息中心一直非常关注网络安全的投资与建设。随着中国黑色产业链的不断发展，病毒、木马等恶意程序对网络、业务系统的危害日益严重，南方电网下属某输电企业信息中心对此也日益关注。因为一旦网络因为病毒导致网络堵塞，多好的电子化业务系统也不能起到任何的效果，还会对全局五省的业务带来严重的后果。因此，早在 2004 年，南方电网下属某输电企业信息中心已经开始对互联网威胁发展以及安全防护新技术进行关注，并希望能够找到一套多层次的安全防护体系，能保障南方电网下属某输电企业业务的顺利开展。

防病毒体系是产品+服务的结合

趋势科技多层次安全防护方案为南方电网下属某输电企业提供全面的安全保障

趋势科技技术顾问与南方电网下属某输电企业信息中心的安全专员进行了深入的沟通，了解到南方电网下属某输电企业的安全威胁主要为以下几点：

Internet 边界访问 －南方电网下属某输电企业与 INTERNET 相连，虽然中间有防火墙验证数据的合法性，但仍会受到来自互联网以 HTTP、FTP 等数据流为载体的潜在病毒的威胁。而且客户机多使用 Windows 操作系统，使用者的不良习惯还无法受到严格约束，一时的疏忽导致病毒感染，再通过其他介质：邮件、文件拷贝，网络传输等手段传播开来，成为病毒在网内感染和蔓延的主要环节。

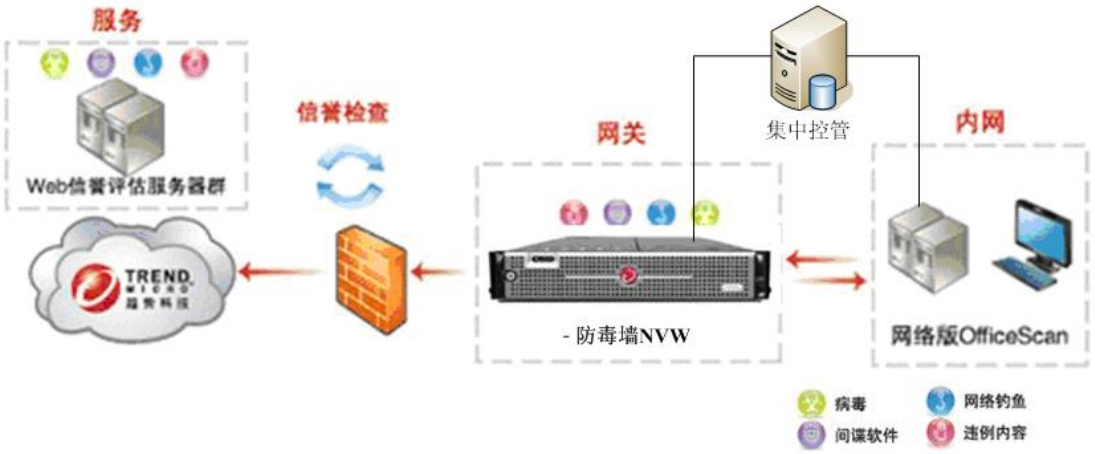
业务网 – 业务网中的 WINDOWS 平台是传播病毒的隐患，其它 LINUX、UNIX 平台通常不会与 Windows 平台交叉感染病毒，传播病毒的可能性也不大。但当客户端网络发起文件访问等数据交互时，病毒有可能通过此渠道进入服务器区段，从而影响业务的运行。

U 盘 – U 盘等移动外设是南方电网下属某输电企业内网病毒交叉感染的主要通道。大量的用户为了工作的方便，会把 U 盘作为办公网、业务网以及家庭 PC 的数据媒体。由于 3 者间的病毒情况根本无法确认，所以病毒就通过这个途径进行扩散。

根据对用户环境、隐患的分析，趋势科技认为，单纯的终端病毒防护体系并不能有效协助南方电网下属某输电企业有效应对新形态病毒的攻击。只有从技术、服务、流程三方面同时加强，才能把南方电网下属某输电企业的安全防护体系全面加固。

产品为基础、服务是保障

在定义了需求后，趋势科技向南方电网下属某输电企业推荐了其历时 2 年半，斥资 3 亿美金研发地“云安全”智能网络防护方案（全网终端防护 Officescan+网络层防护 NVW+全网集中管控 TMCM+趋势科技专家服务）。



- ✓ 第一道防线：在重要的服务器区段边界部署网络防毒墙 NVW，以阻断来自客户端正常网络访问所携带的网络病毒；
- ✓ 第二道防线：在全网所有 windows 终端上部署趋势科技网络版 Officescan，除了利用其病毒码技术进行文件病毒防护外，还利用其独特的云安全 WRS 技术，对客户端访问的站点进行安全性检查，提高内网访问 Internet 的安全性；
- ✓ 第三道防线：由集中控管对所有趋势科技的产品进行集中控管，并由趋势科技提供原厂的专家服务（EOG），以服务为用户保驾护航。

因为考虑到该用户是能够与 Internet 进行数据交互，通过对原有防毒系统的日志分析得知，超过 80%的病毒是通过 Web 进入南方电网下属某输电企业内部网络的。因此，我们在用户网络版 Officescan 上启用业界唯一的 Web 信誉评估技术（WRT），拦截了大量由内部用户发起的对可疑高风险 URL 的访问，大大降低了用户由于访问 URL 带来的风险，避免了因终端使用者安全意识不强，导致的 Web 访问安全问题。

另外，通过有 WRT 对可疑网页访问的拦截，还可以将大部分病毒变种的下载阻断，从而阻止新病毒的入侵，同时也使内网已经存在的病毒无法变种，降低了内网 OfficeScan 客户端的防毒压力。由于 IWSA 部署是采用透明方式，所以，IWSA 的运行既不会对用户日常使用习惯带来影响，同时亦可以保障到用户访问网页的安全。

对于用户担心的 U 盘病毒扩散，通过在全网终端部署 Officescan 来进行防护。Officescan 具备独特的 U 盘病毒自动播放拦截功能，能够在 U 盘接入电脑时，对包含在 U

盘中能够自动注入内存的病毒进行清除，有效提高了南方电网下属某输电企业对 U 盘病毒的控制。

对于用户担心的服务器区段遭受网络病毒攻击，我们特意在服务器区段边界部署趋势科技网络层防毒墙 NVW，对流经 NVW 的所有网络数据包进行检查。一旦发现有网络数据包包含网络病毒，会立刻进行数据包的阻止，并通知管理员是哪台客户端对服务器区段的业务服务器发起攻击，提前预防。

同时，趋势科技还协助南方电网下属某输电企业针对全网防病毒工作建立了一套有效的防病毒处理流程，使全省所有安全管理员在遇到病毒问题的时候，能够按照防病毒处理流程文档进行有序的处理，提高效率。

趋势科技云安全工作原理

趋势科技“云安全”技术是通过多种方式收集数据信息并动态分析恶意威胁，生成动态的 URL，邮件 IP，文件信誉库，并通过行为关联分析技术，建立各种信誉库的关联，当用户访问目标信息时，就可以在几毫秒内与信誉库中的 URL 地址、邮件 IP 地址等进行比对，获得安全访问建议，从源端阻止对不良 URL、邮件和文件的访问，降低网络风险的侵入。目前，“云安全”技术每天接受的用户查询数量已达到 50 亿次，而每日评估处理的 URL、邮件 IP 地址等更达到 1200G，与此同时，因为将 70%威胁特征码放在云端，因此它能够减少企业 PC 70%的核心内存占用，这些是传统的病毒代码比对技术所无法比拟的。

WRT—Web 信誉技术是“云安全”的关键组成部分，旨在 Web 威胁侵害网络或用户的计算机之前对其进行防御。Web 信誉技术为用户访问的网页指定相对的信誉分数，按照

多种指标进行评分，包括网站网页、历史地址变化以及其它可能揭示可疑行为的因素。然后该技术通过恶意行为分析进行深入评估，监督网络流量，识别任何来自 Web 的恶意活动。趋势科技 Web 信誉技术还执行网站内容爬行和扫描，补充对已知恶意或被感染网络的分析结果。然后按照 Web 信誉评分封堵对恶意网页的访问。为了减少误报率、提高准确性，趋势科技的 Web 信誉技术采用细颗粒的评估技术，体现为对具体的网页及其中涉及的各种链接的安全性进行评估，而非促颗粒的对整个站点安全性一刀切的信誉评估，因为有时候合法网站中仅仅只有部分内容遭到攻击。目前，这一“云安全”的核心技术，已经成功应用于趋势科技网关防护产品—Web 安全网关（IWSA）和终端防护产品—趋势科技防毒墙网络版（OfficeScan）之中，成为“云安全”智能防护网络的重要组成部分。